Toolkit for the Differential Cryptanalysis of ARX-based Cryptographic Constructions*

Nicky Mouha[1,2,**], Vesselin Velichkov[1,2,***], Christophe De Cannière[1,2,†], and Bart Preneel[1,2]

[1] Department of Electrical Engineering ESAT/SCD-COSIC, Katholieke Universiteit Leuven. Kasteelpark Arenberg 10, B-3001 Heverlee, Belgium.
[2] Interdisciplinary Institute for BroadBand Technology (IBBT), Belgium.
{Nicky.Mouha,Vesselin.Velichkov,Christophe.DeCanniere}@esat.kuleuven.be

Abstract

We propose a software toolkit, intended to automate the differential cryptanalysis of cryptographic constructions based on the operations addition, rotation and xor (ARX). The toolkit consists of several programs, each of which evaluates the probability that xor or additive differences propagate through a certain type of operation. Types of operations that are supported are xor, modular addition and multiplication by a constant.

A subset of the problems to which the proposed toolkit can be applied, have been studied in literature before. In [1], matrix multiplications are used to calculate the differential probability xdp^+ of addition modulo 2^n, when differences are expressed using xor, and the differential probability $\mathrm{adp}^\oplus$ of xor when differences are expressed using addition modulo 2^n. The time complexity of these computations is linear in the word size n.

In our toolkit, we use the same concept of matrix multiplications. The generated matrices are correct by construction, and their size is automatically minimized. The main advantage of our technique, is that it is more general, and can therefore easily be extended to a larger number of cases. The proposed tools can be used to compute xdp^+ and $\mathrm{adp}^\oplus$, as well as $\mathrm{xdp}^+(\alpha, \beta, \ldots \rightarrow \gamma)$ – the calculation of xdp^+ for more than two inputs, and the differential probability $\mathrm{xdp}^{\times C}$ of multiplication by a constant C where differences are expressed by xor.

The tool is also capable of efficiently counting the number of output differences for each of the mentioned operations. An instance where this problem occurs, is in the cryptanalysis of Threefish-512 [2], where an exponential-in-n time algorithm is proposed. Using the toolkit, this can be solved in linear time in n.

* This work was supported in part by the IAP Program P6/26 BCRYPT of the Belgian State (Belgian Science Policy), and in part by the European Commission through the ICT program under contract ICT-2007-216676 ECRYPT II.
** This author is funded by a research grant of the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen).
*** DBOF Doctoral Fellow, K.U.Leuven, Belgium.
† Postdoctoral Fellow of the Research Foundation – Flanders (FWO).

The tool also provides a general algorithm to efficiently list the output differences with the highest probability, for a given type of difference and operation.

The cases handled by the toolkit, are encountered in many ARX-based cryptographic algorithms. Examples are the XTEA block cipher [3], the Salsa20 stream cipher family [4], and the hash functions MD5 and SHA-1. Other examples are 6 out of the 14 second-round candidates of NIST's SHA-3 hash function competition [5]: BLAKE [6], Blue Midnight Wish [7], CubeHash [8], Shabal [9], SIMD [10] and Skein [11]. Our tools can assist in the cryptanalysis of each of these algorithms.

References

1. Lipmaa, H., Wallén, J., Dumas, P.: On the Additive Differential Probability of Exclusive-Or. In Roy, B.K., Meier, W., eds.: FSE. Volume 3017 of Lecture Notes in Computer Science., Springer (2004) 317–331
2. Aumasson, J.P., Çagdas Çalik, Meier, W., Özen, O., Phan, R.C.W., Varıcı, K.: Improved Cryptanalysis of Skein. In Matsui, M., ed.: ASIACRYPT. Volume 5912 of Lecture Notes in Computer Science., Springer (2009) 542–559
3. Needham, R.M., Wheeler, D.J.: Tea extensions. Computer Laboratory, Cambridge University, England (1997) `http://www.movable-type.co.uk/scripts/xtea.pdf`.
4. Bernstein, D.J.: The Salsa20 Family of Stream Ciphers. In Robshaw, M.J.B., Billet, O., eds.: The eSTREAM Finalists. Volume 4986 of Lecture Notes in Computer Science. Springer (2008) 84–97
5. National Institute of Standards and Technology: Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family. Federal Register **27**(212) (November 2007) 62212–62220 Available: `http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf` (2008/10/17).
6. Aumasson, J.P., Henzen, L., Meier, W., Phan, R.C.W.: SHA-3 proposal BLAKE. Submission to the NIST SHA-3 Competition (Round 2) (2008)
7. Gligoroski, D., Klima, V., Knapskog, S.J., El-Hadedy, M., Amundsen, J., Mjølsnes, S.F.: Cryptographic Hash Function BLUE MIDNIGHT WISH. Submission to the NIST SHA-3 Competition (Round 2) (2009)
8. Bernstein, D.J.: CubeHash specification (2.B.1). Submission to the NIST SHA-3 Competition (Round 2) (2009)
9. Bresson, E., Canteaut, A., Chevallier-Mames, B., Clavier, C., Fuhr, T., Gouget, A., Icart, T., Misarsky, J.F., Naya-Plasencia, M., Paillier, P., Pornin, T., Reinhard, J.R., Thuillet, C., Videau, M.: Shabal, a Submission to NIST's Cryptographic Hash Algorithm Competition. Submission to the NIST SHA-3 Competition (Round 2) (2008)
10. Leurent, G., Bouillaguet, C., Fouque, P.A.: SIMD Is a Message Digest. Submission to the NIST SHA-3 Competition (Round 2) (2009)
11. Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J., Walker, J.: The Skein Hash Function Family. Submission to the NIST SHA-3 Competition (Round 2) (2009)